STATE OF ALABAMA

Information Technology Standard

Standard 640-02S4: Remote Maintenance

1. INTRODUCTION:

Information systems must have security controls in place to protect the routine remote maintenance activities that enable the system to function correctly. These activities include diagnosing and fixing software or hardware problems; loading, maintaining, and updating software, firmware, device drivers, configuration settings, etc., and maintaining a historical record of system changes. The following controls address remote access to information systems for the purpose of remote maintenance activities.

2. OBJECTIVE:

Manage and monitor remotely executed maintenance and diagnostic activities.

3. SCOPE:

These requirements apply to all personnel (State employees, contractors, vendors, and business partners) who access any State of Alabama information system resources for the purpose of performing remote maintenance and diagnostic activities.

4. REQUIREMENTS:

The following State of Alabama requirements are based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-53: Recommended Security Controls for Federal Information Systems.

4.1 REMOTE MAINTENANCE

Log all remote maintenance, diagnostic, and service activities. Maintenance logs should be reviewed daily, but shall be reviewed at least weekly.

Describe the use of remote diagnostic tools, and address the installation and use of remote diagnostic links, in system security plans.

Apply security controls (e.g., authorization, authentication, encryption, etc.) to the remote maintenance access connection in accordance with applicable State standards.

Whenever possible, utilize two-factor authentication on remote maintenance ports.

Ensure that remote maintenance access is normally blocked unless unattended access is required. Whenever possible, require some involvement of local personnel in opening remote maintenance ports.

Keep maintenance terminals in locked, limited-access areas.

Whenever possible, turn off maintenance features when not needed.

When remote maintenance is completed terminate all sessions and remote connections. If password-based authentication was used during remote maintenance, change the passwords following each remote maintenance service.

If remote diagnostic or maintenance services are required from a service or organization that does not implement for its own diagnostic or maintenance systems the same level of security as that implemented on the system being serviced, the system being serviced shall be sanitized and physically separated from other information systems before the maintenance connection is made. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.

4.2 MAINTENANCE PERSONNEL

Ensure that only personnel authorized in writing by the IT Manager or system owner perform maintenance on the information system. Maintain a list of authorized maintenance personnel.

When maintenance personnel do not have the needed access authorizations, organizational personnel with appropriate access authorizations shall supervise maintenance personnel during the performance of maintenance activities on the information system.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 640-02: Remote Access

6.2 RELATED DOCUMENTS

Signed by Eugene J. Akers, Ph.D., Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	2/16/2007	